Introduction to Computer Security
Midterm Exam
Fall 2006

This is a closed-book, closed-notes exam. All problems have equal weight.

1. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Access Control Matrix

   (b) Common Criteria

   (c) Originator controlled access control

   (d) Capability based access control

   (e) Lampson's definition of a storage channel

2. Information-flow security [30 points]

   Consider the six program fragments:

```
 1   l := h
 2   h := l
 3   l := false; if h then l := true else skip
 4   h := false; if l then h := true else skip
C1       l := false;
         while h do l := true
C2       l := false;
         while h do skip;
         l := true
```

(a) Assume `h > l`. Explain informally which flows are desired and which flows should be prevented (undesired flows).

(b) Which flows are explicit (direct in the study questions); which are implicit (indirect)?

(c) Use the Sabelfeld and Myers type system to show that three of these programs are typable and three are not.

(d) Volpano, Smith and Irvine define two properties, *simple security* and *confinement*. Simple security says that, when $\vdash e : \tau$, "only variables at level τ or lower in e will have their contents read when e is evaluated (no read up)." Confinement says that, when $[\tau] \vdash c$ "no variable below level τ is updated in c".

For each program fragment, discuss if it violates these properties.

(e) Consider program fragments C1 and C2. Did the type system get the right answer? Discuss any anomalies concerning C1 and C2 in your answers above.

(f) Bishop's presentation gives a rule for while loops that requires that each loop terminates. This condition is omitted in the Sabelfeld and Myers system presented in class. Does Bishop's requirement that all while loops terminate eliminate any anomalies? Discuss.

3. Basic Principles and Voting Machines [15 points]

(a) In English, state the security policy for a voting system. Identify which requirements address confidentiality, integrity, and availability concerns.

(b) Summarize the vote stealing attack presented in the Feldman, Halderman, and Felten paper.

(c) What aspects of the security policy does the vote stealing attack violate?

(d) Feldman, Halderman, and Felten also sketch denial of service attacks; describe a denial of service attack on the Diebold voting machine.

(e) What aspects of the security policy does the denial of service attack violate?

4. Integrity Model applied to Voting Machine [40 points]

   This question has been modified since being released as a study question.

   You are being asked to re-engineer the voting machine that Felten's lab studied. To increase assurance you have been asked to apply the Biba integrity model to the design.

   In the new design you are to implement four distinct levels of integrity, corresponding to the following agents:

Agent	Level	Abbreviation
Trusted Vendor	TCB	T
System Administrator	Admin	A
Election Official	Official	O
Voter	Voters	V

   The levels are listed in order from most trusted (T) to least trusted (V).

   You have learned that the smart card reader/writer is a trustworthy device. You can trust this unit to authenticate users of the system. In particular, each smart card indicates what kind of agent is authentication (T, A, O or V), and for all agents except voters provides a reliable unique identity.

   System Components:

   - Hardware
     - Processor
     - EPROM
     - On-board flash
     - Removable Flash (key access)
     - Printer (key access)
     - Smart card reader/writer (open)
     - Display (open)
   - Key files
     - Boot loader
     - Operating System
     - Task Manager
     - Voting Software
     - Vote Tally
   - Logical Operations
     (a) **Update boot loader**
     (b) Update OS and applications
     (c) **Define Ballot**

(d) Start election

(e) **Vote**

(f) End election

(g) **Post-election reporting**

(a) [5 points] Elaborate the Biba integrity model for this system by assigning integrity levels to all key files. Specifically assign integrity levels for creating or modifying these files.

(b) [5 points] Several known exploits of the system rely on infection via removable media. Propose a mechanism that uses the trusted authentication mechanism and integrity model to prevent these exploits.

(c) [5 points] Argue that the intended operations listed above in **bold face** can be carried out by appropriate subjects without violating the policy. If it is necessary to specify that any software run at a higher level of integrity than the currently authenticated user please note which software and what level of integrity is should assume.

(d) [5 points] Argue that with these mechanisms and a faithful implementation of the integrity model that Felten's vote stealing and denial of service attacks would not be allowed.

(e) [5 points] Having developed this design, it is now time to critique it! Are you satisfied with the protection against external threats? Are you satisfied with the protection against insider threats? Discuss.

(f) [5 points] If the Clark-Wilson model were applied, the vote tally would be a constrained data item (CDI) and voting would be a transaction process (TP).

What audit requirements would be dictated by these designations?

(g) [5 points] Are these requirements in conflict with the confidentiality policy expected of a voting machine?

(h) [5 points] Suggest a mechanism that balances the need for audit requirement with the confidentiality policy.